LepideAuditor

Enable Logon/Logoff Events Monitoring

Table of Contents

1. Introduction

This helpful guide takes you through the necessary steps to enable the auditing of logon/logoff events. In both agentless and agent-based auditing, the following steps must be completed:

- Generate "Logon.exe" from the software, while adding or modifying the domain, and create a Group Policy on the server to assign it. It will collect logon and logoff events and passes them to Logon/Logoff Audit Module.
- Install Logon/Logoff Audit Module on any of the domain controllers of the domain, which will process logon/logoff events and send it to the software for display.

Both of these modules should run continuously at the server for collecting logon/logoff events. The following items will not be generated if the above steps are not performed.

- "Successful User Logon/Logoff" and "Domain Controller Logon/Logoff" Reports
- Custom Reports, LiveFeed, alerts, and scheduled reports for above reports

2. Issue

If you have neither installed Logon/Logoff Audit Module nor generated “logon.exe” nor linked it with the server, the following error appears onscreen while generating "Successful User Logon/Logoff" or "Domain Controller Logon/Logoff".

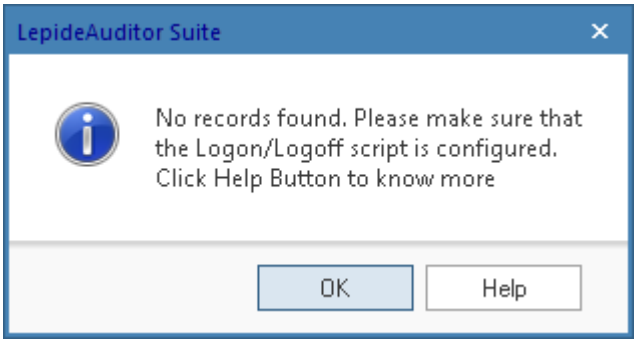

Figure 1: Error while generating logon/logoff reports

You have to generate logon.exe, link it with a Group Policy, and install Logon/Logoff Audit Module to enable the auditing of logon/logoff events to fix this issue.

3. Manage Logon/Logoff Audit Module

The steps to install, manage, and uninstall the logon/logoff Audit Module are listed here.

3.1 Install Logon/Logoff Audit Module

To audit logon/logoff events, you will need to install LepideAuditor Logon/Logoff Audit Module on any of the domain controllers of the domain to collect logon/logoff events. The installer file for this module will come with setup file, which you can download from http://www.lepide.com/lepideauditor/download.html. After downloading this installer file, execute the following steps to install the Logon/Logoff Audit Module.

1. Double-click the downloaded installer file to start the installation.
2. Click "Next" to proceed to the next step of the license agreement.
3. It is recommended to read the license agreement carefully before installing the software.
4. If you agree to the license agreement and want to continue with the installation, check "I accept the agreement" and click "Next".
5. The next step lets you customize the location of the shortcuts folder in the Start Menu.
6. Click "Browse" and select a different location to modify the location of the shortcuts folder in the Start Menu.
7. Click "Next" to use the default or customized shortcuts folder.
8. Check the boxes titled "Create a desktop icon" and/or "Create a Quick Launch icon", if you want.
9. Click "Next" to proceed further. The software is now ready to be installed.
10. Click "Install" to begin the installation procedure.
11. Once installed, the following page comes in the wizard. It asks for the login credentials of a user having administrative privileges.

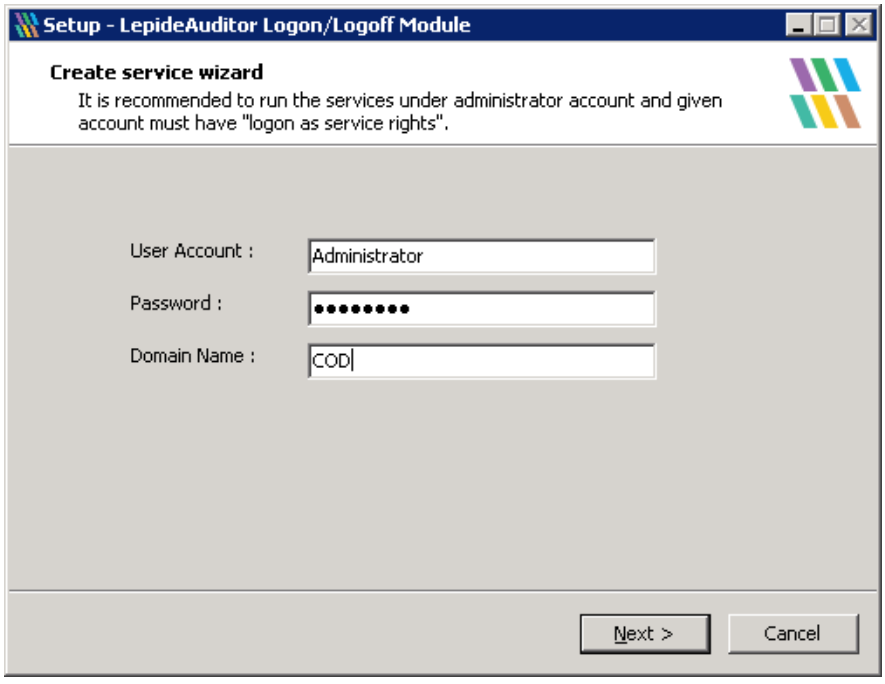

Figure 2: Asking for login credentials of an administrator to create the service

12. Enter the login credentials of a local administrator, domain administrator or a Managed Service Account object on this page. Leave the password text box blank when you select to enter the name of a Managed Service Account object.

NOTE: You should use any of the following account or object.

1. A local system administrator
2. A member of Domain Admins Group
3. Manage Service Account object

13. Click "Next" after entering the login credentials of an administrator. The next page displays the message of successful installation of the module.
14. Click "Finish" to complete the process.

3.2 Stop Logon/Logoff Module

You may have to stop the app server either to stop receiving logon/logoff events or to uninstall the Module. Perform the following steps.

1. Go to "Start Menu" → "Administrative Tools" → "Services" to access the services.
2. Locate "Lepide Logon Logoff Service". Right-click on it to access the context menu.
3. Click "Stop" to stop the service.

3.3 Uninstall Logon/Logoff Audit Module

Execute the following steps.

1. There are two ways to start the uninstallation.
   a. Go to Start → All Programs → "LepideAuditor Logon/Logoff Audit Module", click "Uninstall LepideAuditor Logon/Logoff Audit Module".
   b. Go to Start → Control Panel → "Add/Remove Programs" or "Programs". Select "LepideAuditor Logon/Logoff Audit Module" and click "Remove".

   Following any of the above methods displays a warning message.
2. Click "Yes" to uninstall the module. After completing the uninstallation, the message box appears.
3. Click "OK" to complete the process.

4. Generate Logon.exe file

Perform the following steps on software to generate "logon.exe" file.

1. Use any of the following methods to start with this process.

A. While adding a domain with Advanced Configuration, you arrive at the following step.

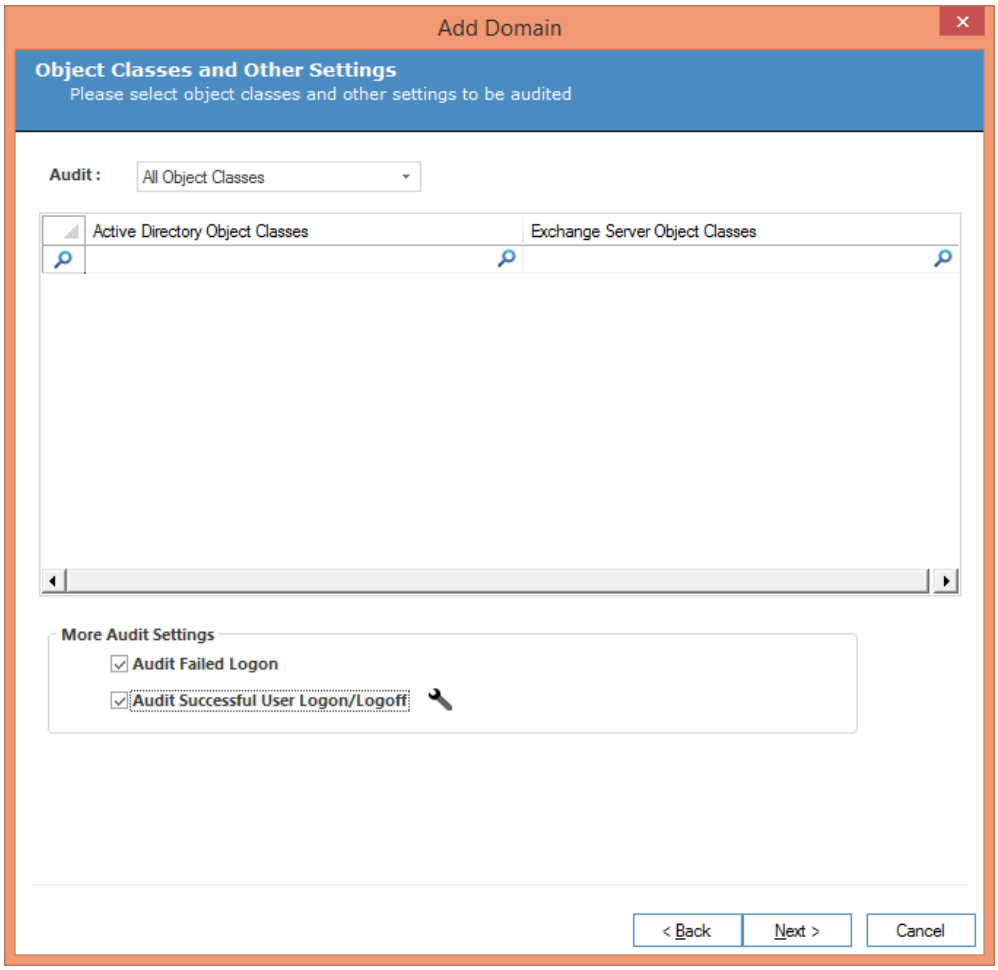

Figure 3: Advanced Domain Configuration

B. In domain properties, go to "Object Class and Other Settings" to access the following settings.

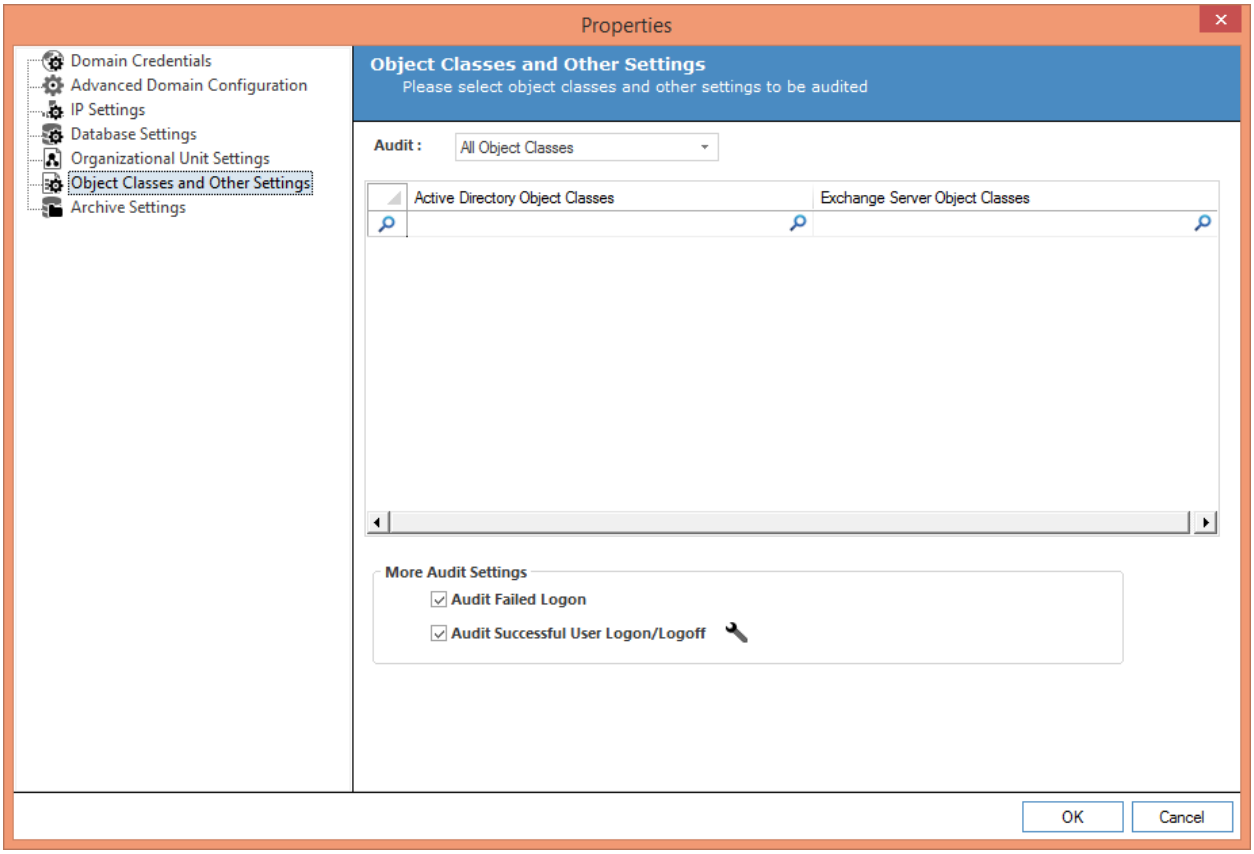

Figure 4: Modifying Object Class and other Settings

2. Check "Audit Successful User Logon/Logoff" option.
3. Click icon to access the following dialog box.

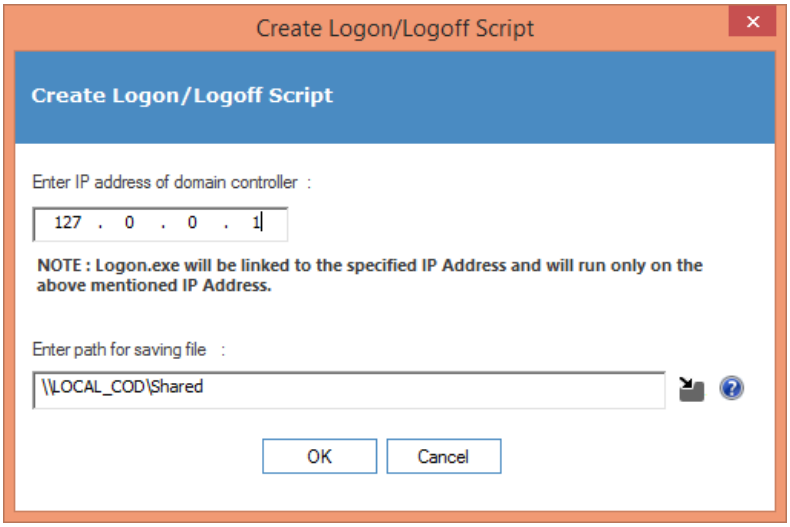

Figure 5: Dialog box to create logon/logoff script

4. Enter the IP Address of the domain controller, where Logon/Logoff Audit Module has been installed.
5. Click icon to select the location on the server to the save this executable file.

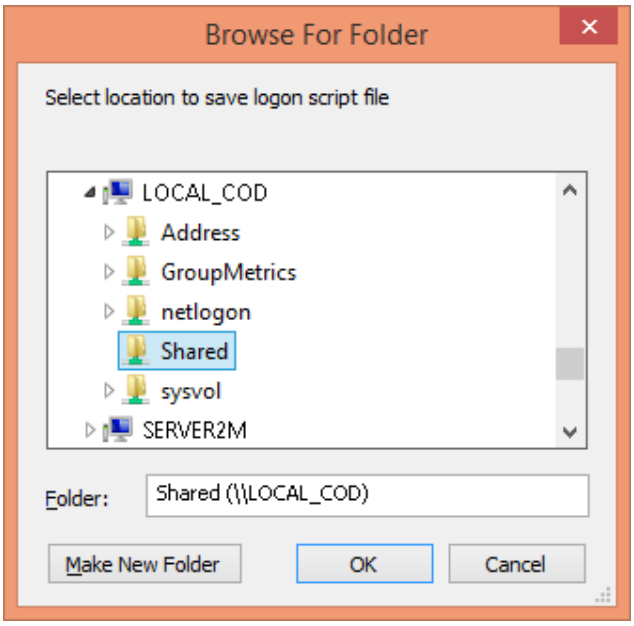

Figure 6: Browse for Server

It is recommended to save the executable file in the shared folder on the server, of which logon/logoff events you want to monitor.

6. Select the folder.
7. Click "OK" to go back to the previous dialog box, which now shows the selected folder.
8. Click "OK" to generate and save the executable file to the specified location. The following message appears on the screen to confirm the same.

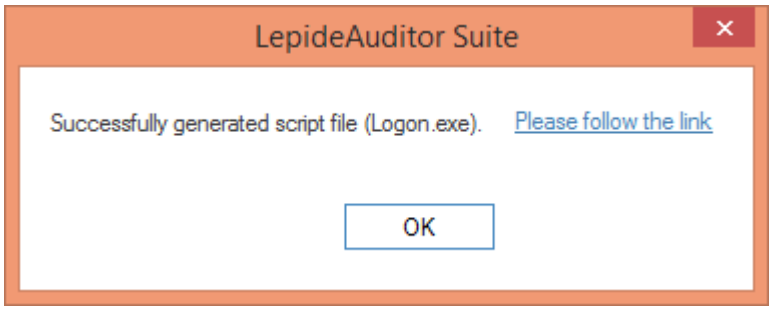

Figure 7: Successfully generated executable file

9. Click hyperlink titled "Please follow the link" to know the steps to be performed at the server. It opens an HTML file in the default Web Browser.

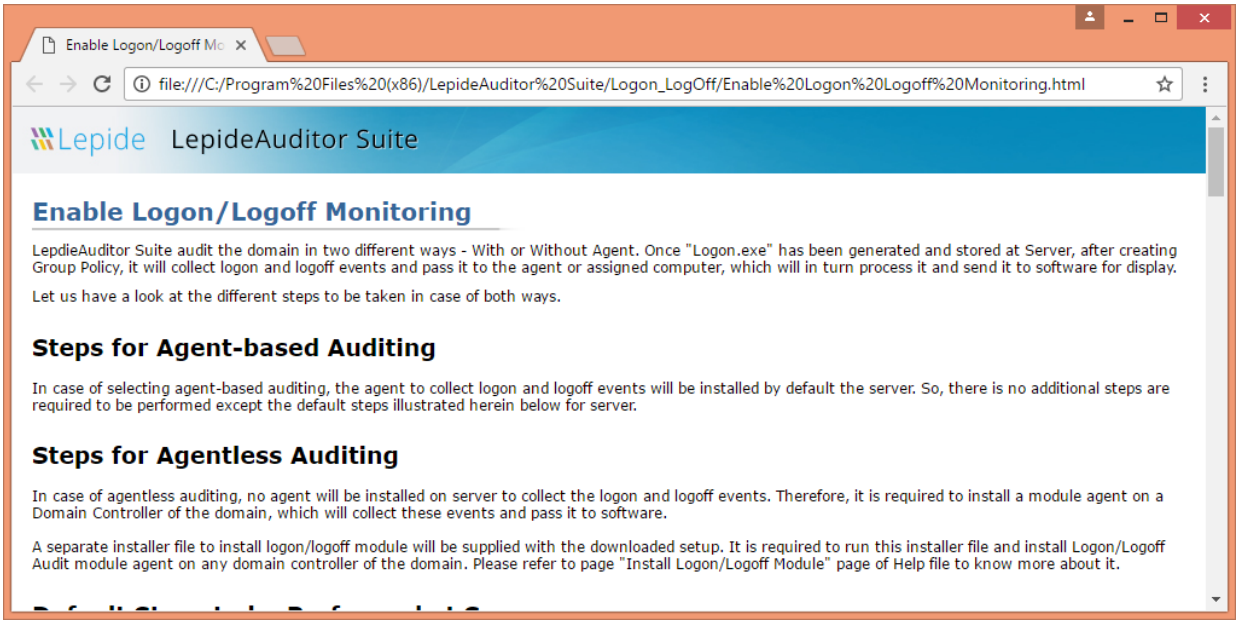

Figure 8: Document showing further steps to be performed

5. Create Group Policy Object at Server

Execute the steps below at the domain, of which logon/logoff monitoring you want to enable.

1. Go to "Start Menu" → "All Programs" → "Administrative Tools" → "Group Policy Management". It opens "Group Policy Management".

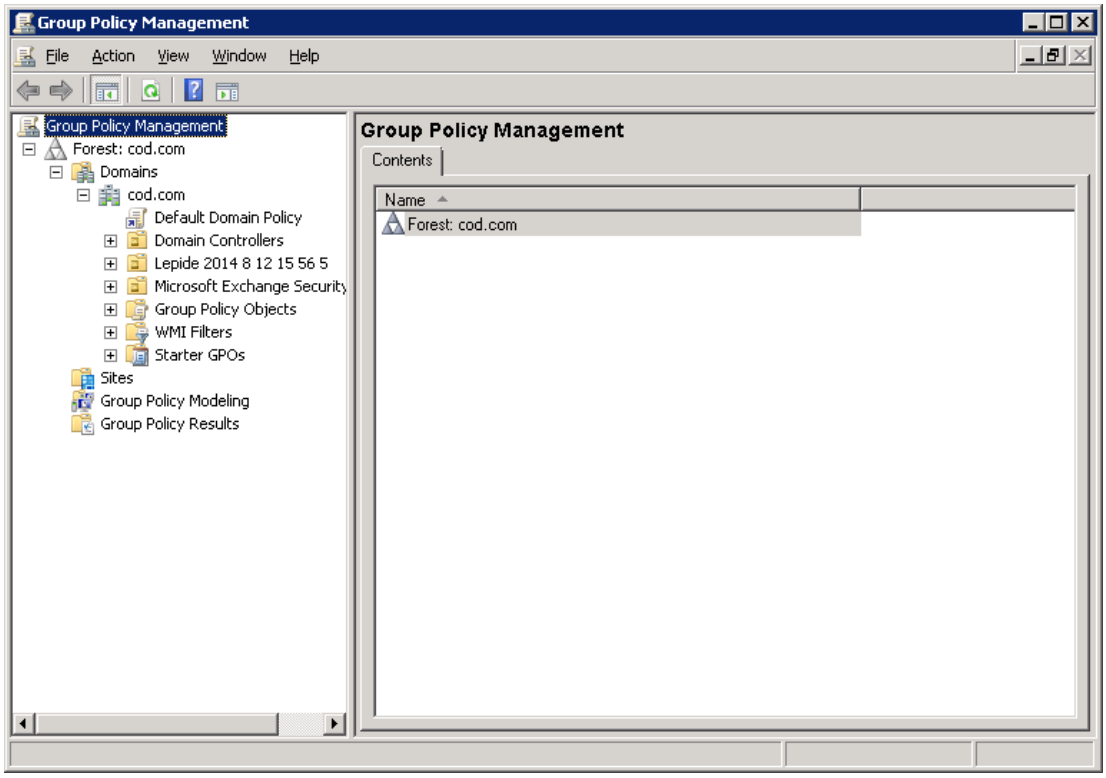

Figure 9: Group Policy Management

2. In the left panel, expand the nodes to reach the node of the domain controller.
3. Right click on the node of the domain to access the following context menu.

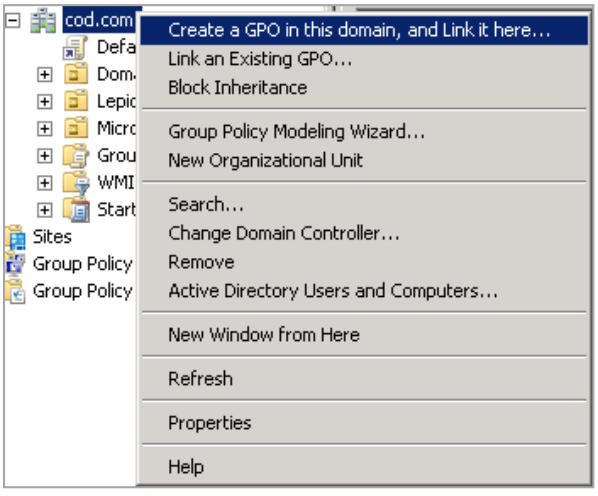

Figure 10: Context Menu for a DC in Group Policy Management

4. Select the option "Create a GPO in this domain, and Link here...". It displays the following dialog box to create a new Group Policy Object (GPO).
5. Provide a name for the new Group Policy e.g. "Logon Logoff by LepideAuditor".

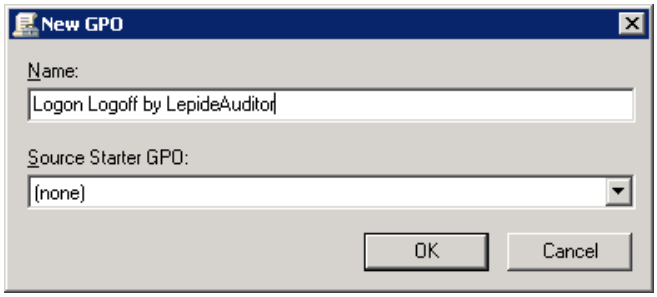

Figure 11: Providing a name for the GPO

6. Click "OK". It creates the new GPO and shows it in the Group Policy Management.

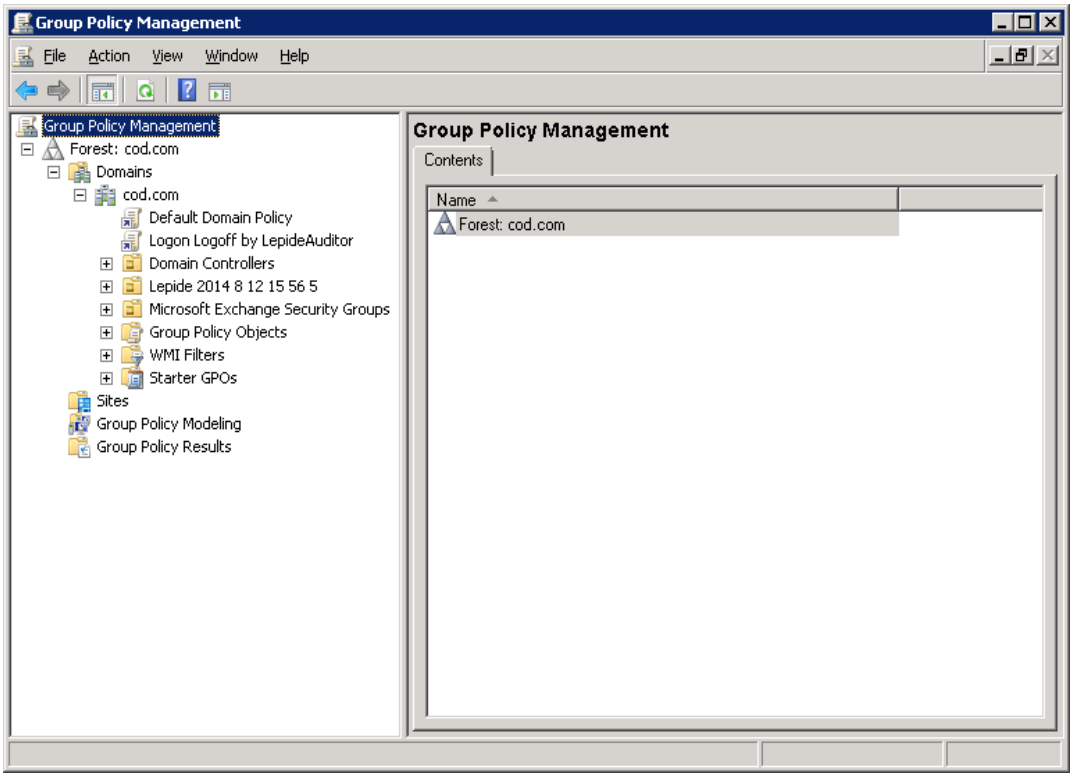

Figure 12: Showing the newly created GPO

7. Right-click newly created GPO.

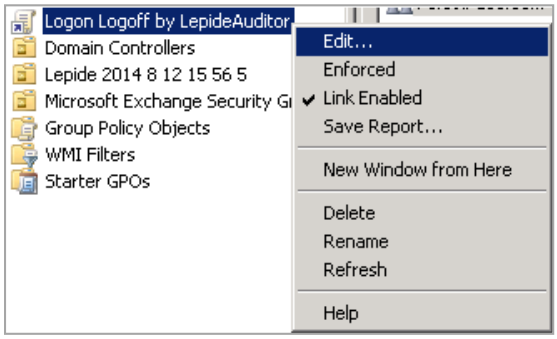

Figure 13: Right Click Menu for the new GPO

8. Click "Edit" to access “Group Policy Management Editor” console.

9. In the left panel, go to "Logon Logoff by LepideAuditor" → "User Configuration" → "Policies" → "Windows Settings" → Scripts (Logon/Logoff)". It displays two policies – “Logon” and “Logoff” in the Right Panel.

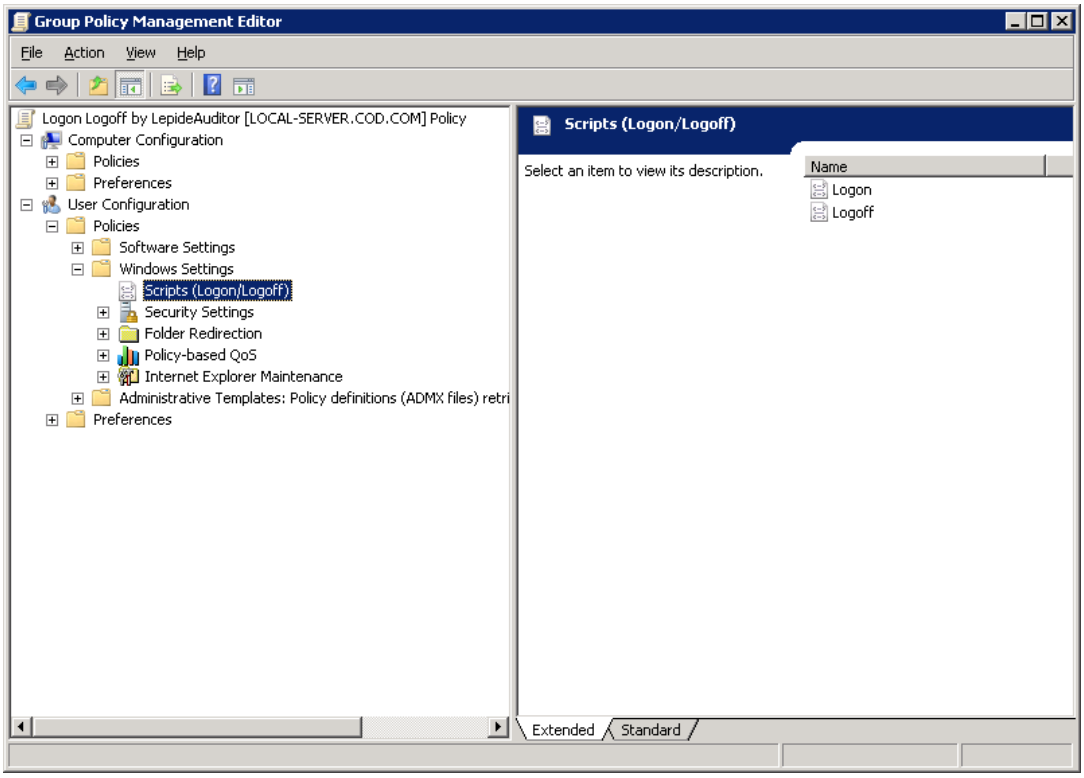

Figure 14: Showing Logon and Logoff Policies

10. Here, you have to modify any of these two policies. In this test case, we are modifying the logon policy.

11. Double-click "Logon" policy in the Right Panel to access the following dialog box.

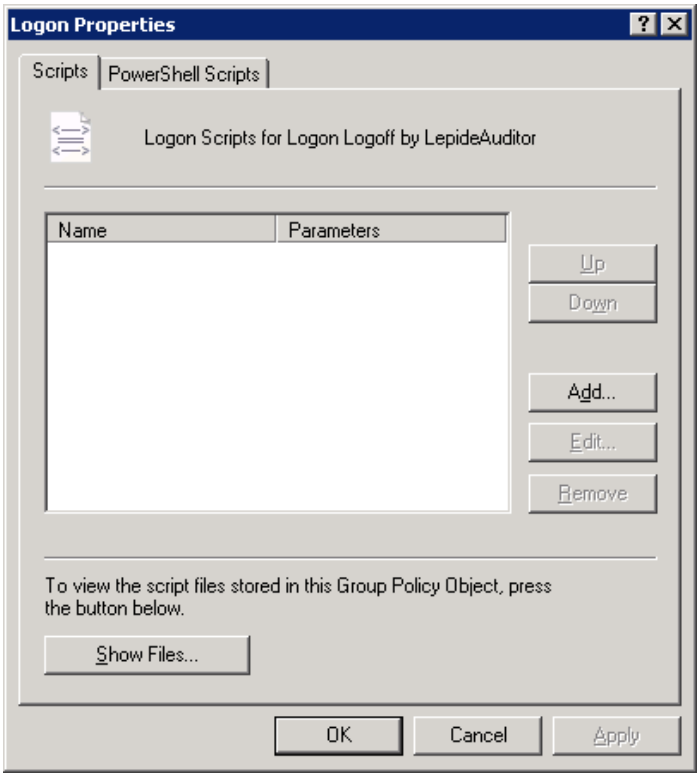

Figure 15: Logon Properties

12. Click "Add" on this tab. It displays the following box to add a script.

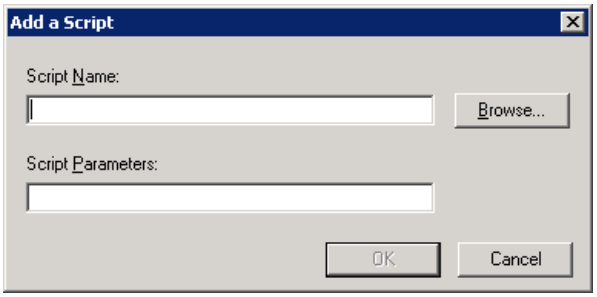

Figure 16: Dialog box to add a logon script

13. Click "Browse" in this new box. Leave this box opened up as it is.

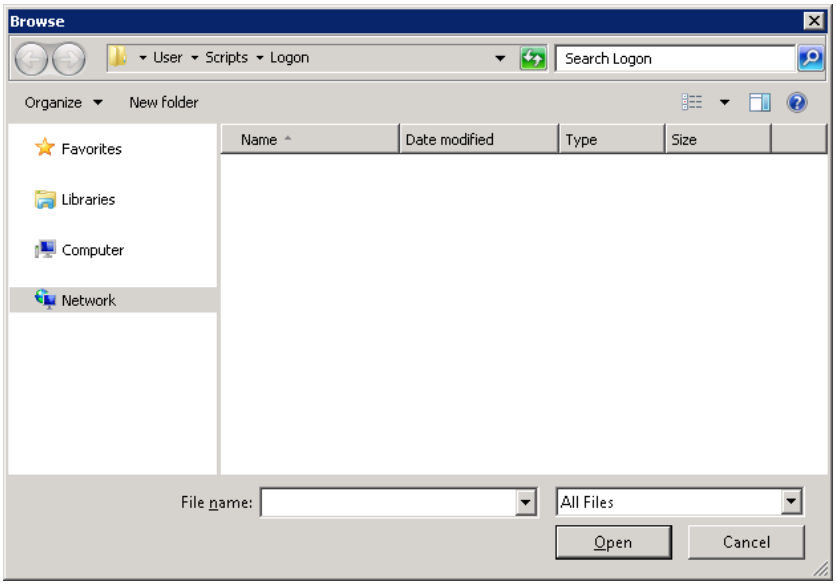

Figure 17: Dialog box to open a logon script file

14. Open the shared folder where you have copied the "Logon.exe" script file. Copy it.

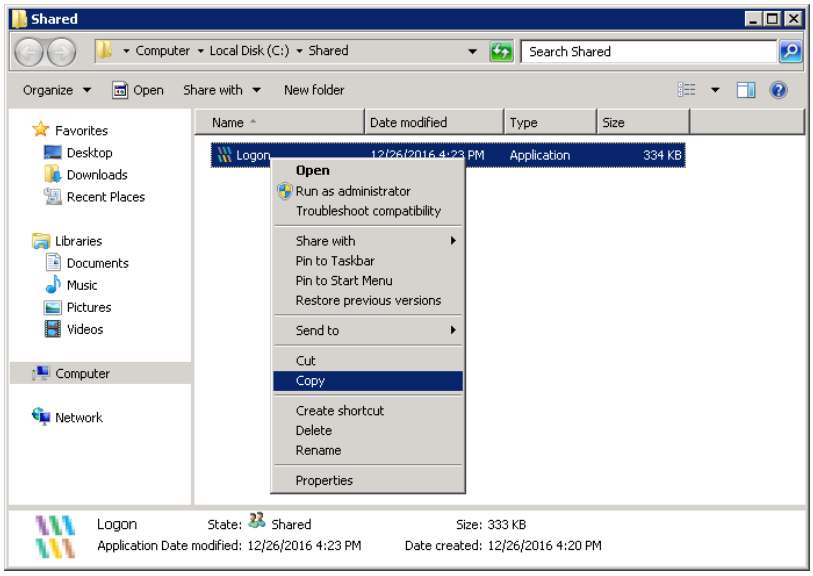

Figure 18: Copying file "Logon.exe

15. Paste this file "logon.exe" in the folder section of the "Browse" window.

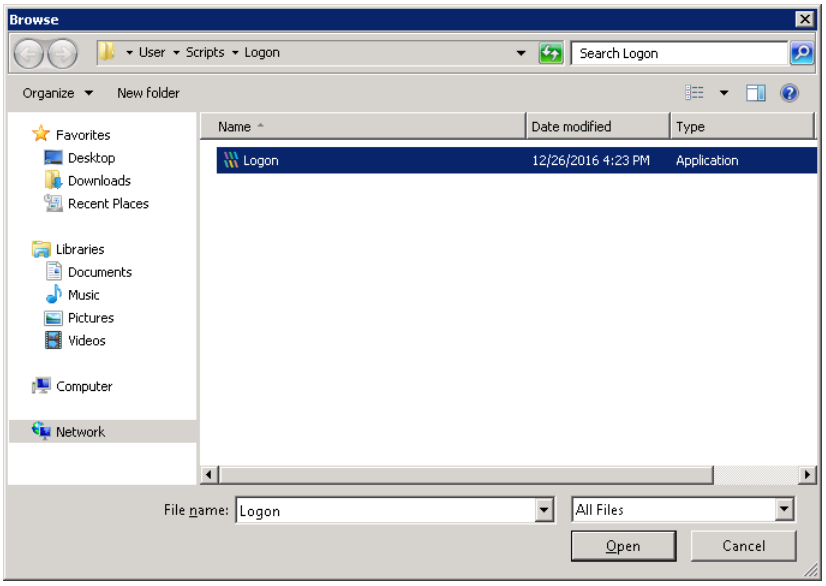

Figure 19: Pasted the file named "Logon.exe

16. Select the file and click "Open". It opens the file and takes you back to the "Add a Script" box, which now displays the selected file.

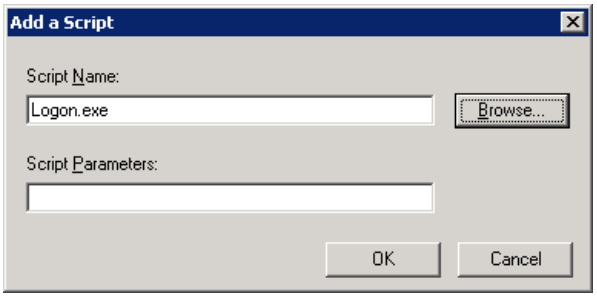

Figure 20: File has been selected

17. Click "OK". It takes you back to the "Logon Properties".

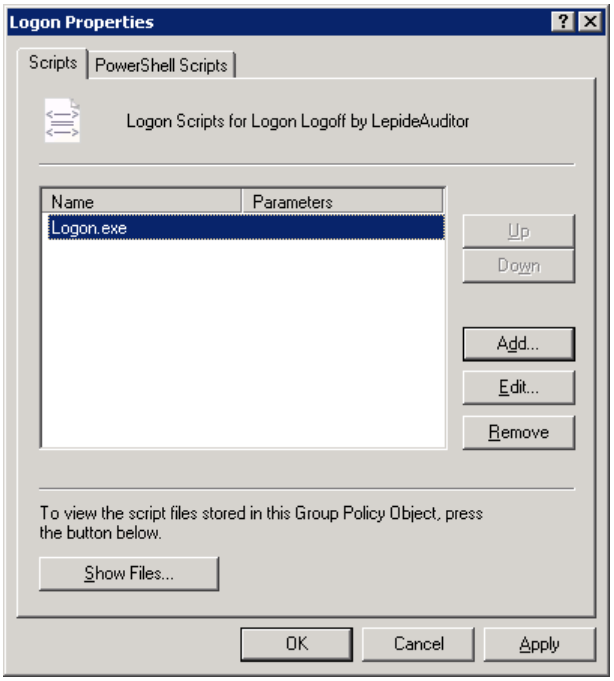

Figure 21: Required Logon Properties

18. Click "Apply" and "OK" to apply the changes.
19. By default, this "logon.exe" is set to run late during the system startup. The steps to avoid this delay are explained in the following methods.
    a. Steps for Windows Server 2016 and Windows Server 2012 R2:

       It is required to perform the following steps to remove this delay in running logon.exe.

       i. In the same Group Policy Management Editor, go to "Computer Configuration" → "Policies" → "Administrative Templates" → "System". Select "Group Policy" node under "System". It shows all of its sub-policies in the right panel.

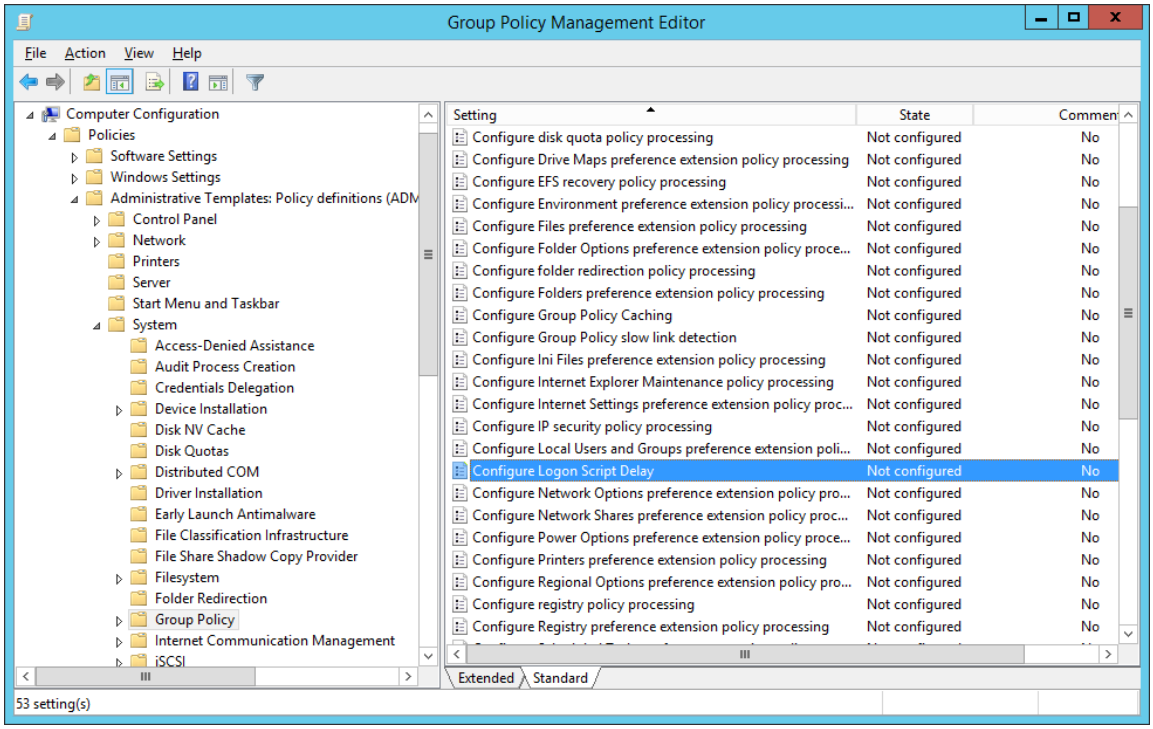

Figure 22: List of Policies in "Group Policy" Category under "System"

ii. Double-click "Configure Logon Script Delay" to access its properties.

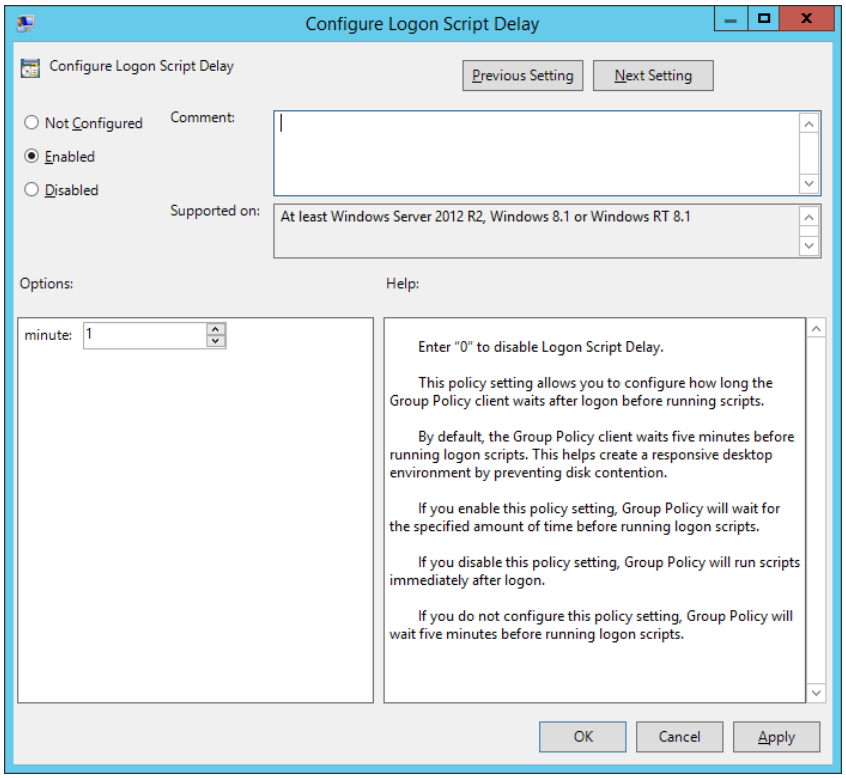

Figure 23: Configure Logon Script Delay Policy

iii. Click "Enabled".

iv. Enter the value as "1" to run the logon scripts after one minute of the logon.

v. Click "Apply" and "OK".

b. **Steps for Windows Server 2008 R2, Windows Server 2008, Windows Server 2012:**

i. It is required to perform the following steps to remove this delay in running logon.exe.

ii. In the same Group Policy Management Editor, go to "Computer Configuration" → "Policies" → "Administrative Templates" → "System". Select "Scripts" node under "System". It shows all of its sub-policies in the right panel.

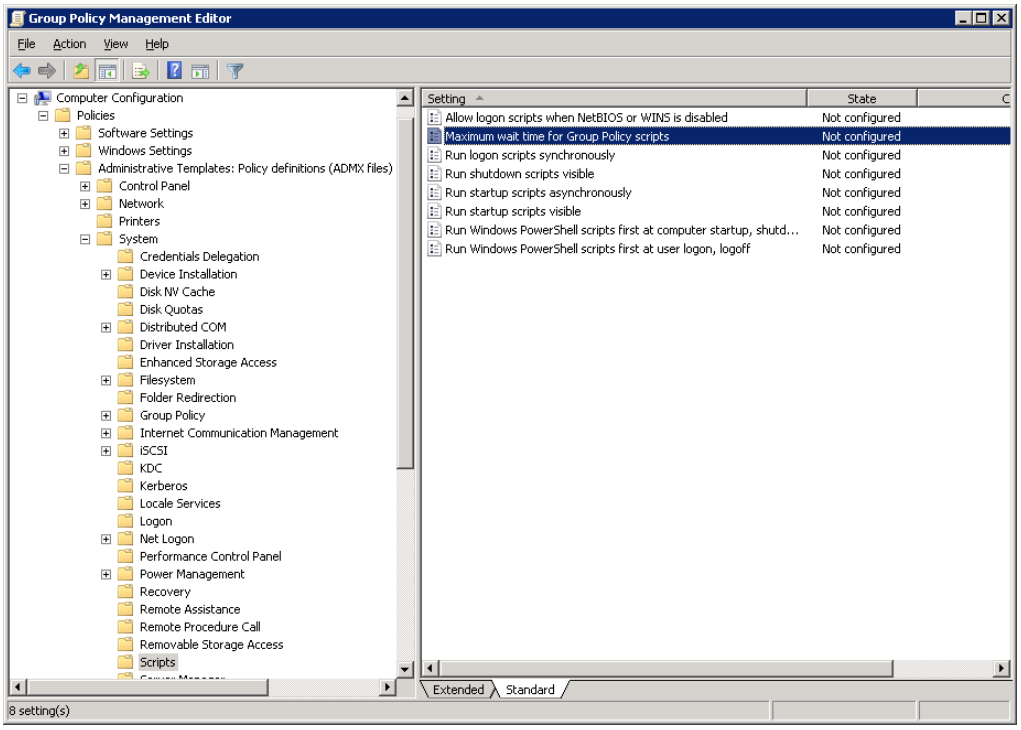

Figure 24: List of policies in "Scripts" category

iii. Double-click "Maximum wait time for Group Policy Scripts" to access its properties.

NOTE: In Windows Server 2012, this policy is available as "Specify Maximum wait time for Group Policy Scripts".

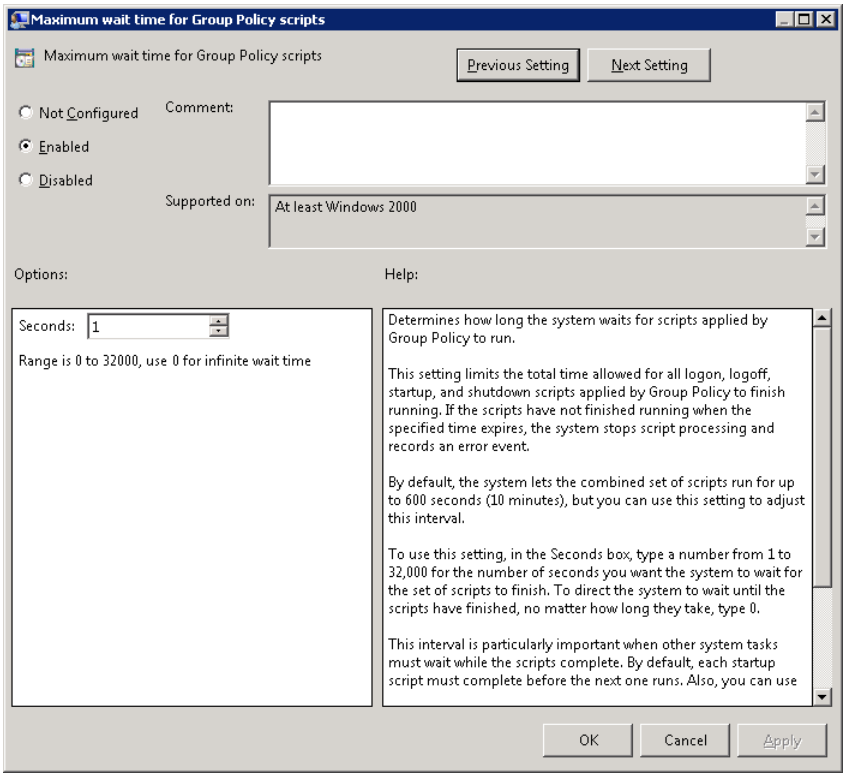

Figure 25: "Maximum wait time for Group Policy scripts" policy

iv. Click "Enabled".

v. Enter the value for seconds. The idle value is 1 second.

vi. Click "Apply" and "OK".

20. Close "Group Policy Management Editor" console.
21. Come back to "Group Policy Management" console.
22. Select the newly created/modified policy in the Left Panel. It shows its details in the Right Panel.

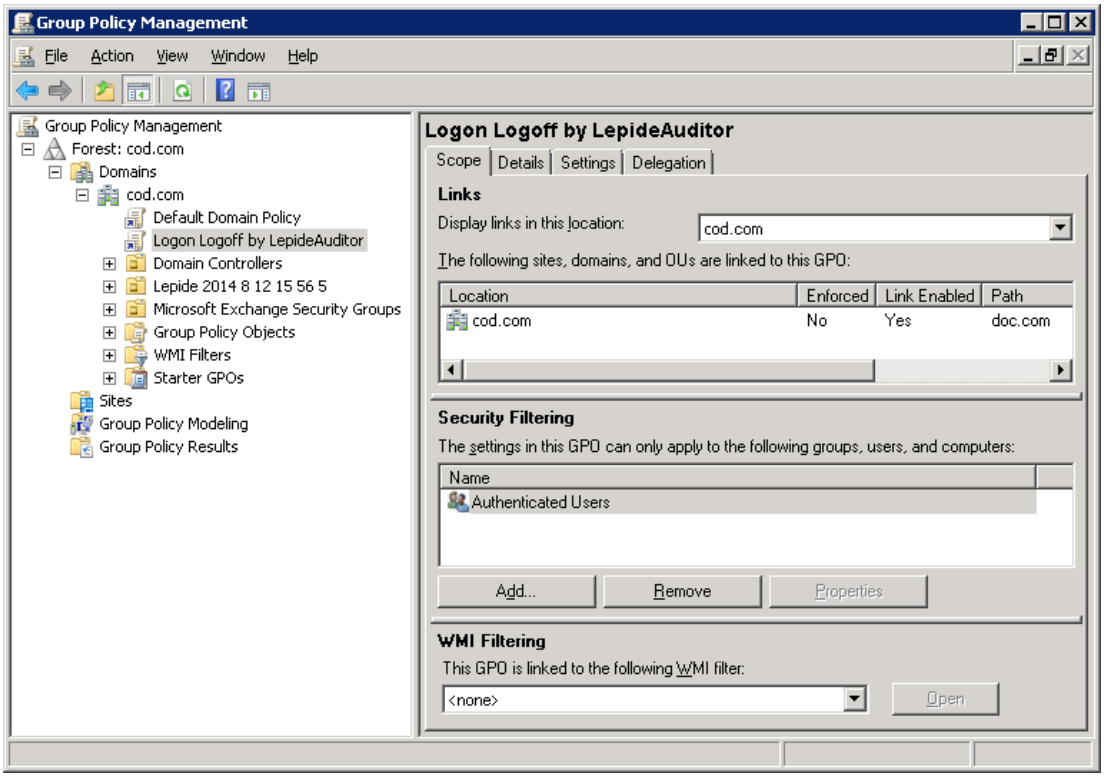

Figure 26: Showing the properties of newly created policy

23. In its Right Panel, the "Security Filtering" section lets you select the objects such as users, groups, and computers on which this policy will be applied.
24. Click "Add" to display the box to add the objects upon which this policy will be applicable.

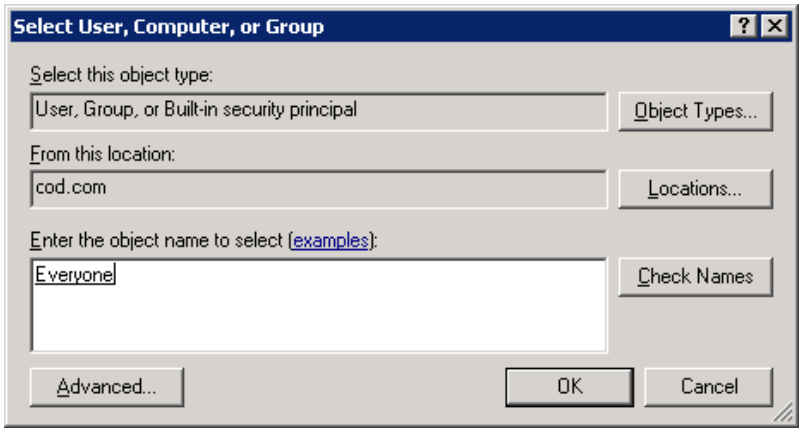

Figure 27: Select the objects to be affected by this policy

25. Type "Everyone" in the text box and click "Check Names". It selects all objects.
26. Click "OK" to confirm the change. It takes you back to the "Group Policy Management" window, which now displays the newly added object.

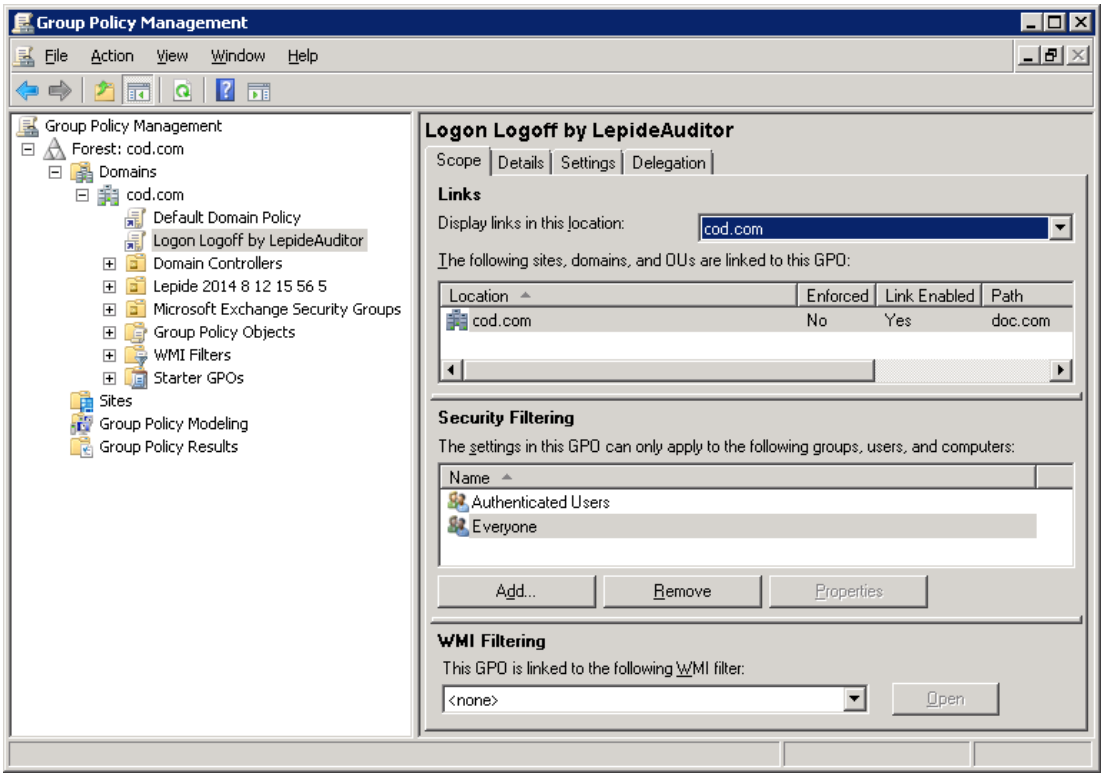

Figure 28: Showing 'Everyone' in Security Filtering

27. Close the "Group Policy Management" console.
28. Go to Run or Command Prompt and type the command "gpupdate".
29. Press Enter to run the "gpupdate" command to update the group policies.

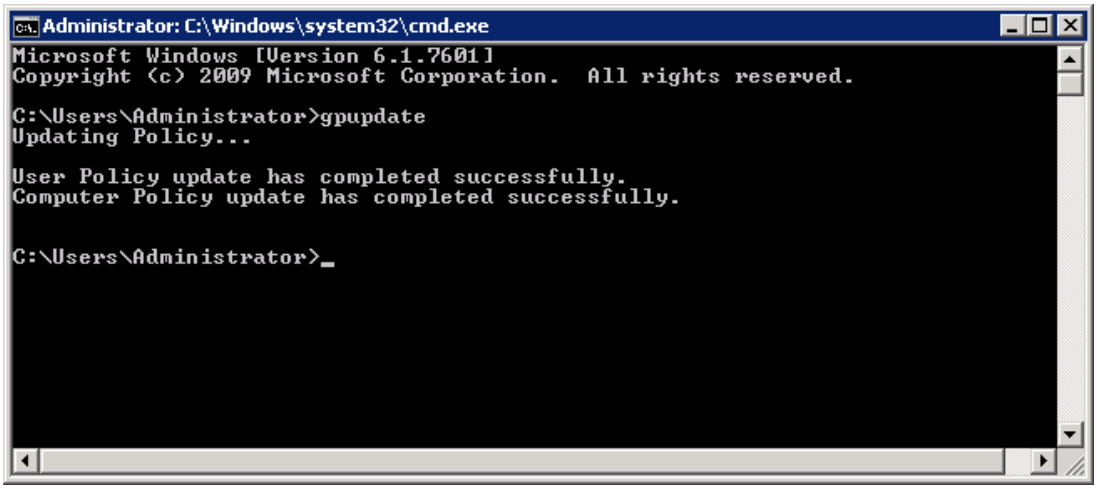

Figure 29: Updated the Group Policies successfully

30. It is required to logoff the current user and then logon again in the Windows Server to run “logon.exe” file.

You can follow the above steps to enable both the collection of logon/logoff events and to generate relevant reports, alerts, and LiveFeed updates.

6. Support

If you are facing any issues whilst installing, configuring or using the solution, you can connect with our team using the below contact information.

Product experts

USA/Canada: +1-800-814-0578

UK/Europe: +44 (0) -845-594-3766

Rest of the World: +91 (0) -991-004-9028

Technical gurus

USA/Canada: +1-800-814-0578

UK/Europe: +44(0)-800-088-5478

Rest of the World: +91(0)-991-085-4291

Alternatively, visit http://www.lepide.com/contactus.html to chat live with our team. You can also email your queries to the following addresses:

sales@Lepide.com support@Lepide.com

To read more about the solution, visit http://www.lepide.com/lepideauditor/.

7. Copyright

8. Warranty Disclaimers and Liability Limitations

LepideAuditor, LepideAuditor App, LepideAuditor App Server, LepideAuditor (Web Console), LepideAuditor Logon/Logoff Audit Module, any and all components, any and all accompanying software, files, data, and materials are distributed and provided AS IS and with no warranties of any kind, whether expressed or implied. In particular, there is no warranty for any harm, destruction, impairment caused to the system where these are installed. You acknowledge that good data processing procedure dictates that any program, listed above, must be thoroughly tested

with non-critical data before there is any reliance on it, and you hereby assume the entire risk of all use of the copies of LepideAuditor and the above listed accompanying programs covered by this License. This disclaimer of warranty constitutes an essential part of this License.

In no event does Lepide Software Private Limited authorize you or anyone else to use LepideAuditor and the above listed accompanying programs in applications or systems where LepideAuditor and the above listed accompanying programs' failure to perform can reasonably be expected to result in a significant physical injury, or in loss of life. Any such use is entirely at your own risk, and you agree to hold Lepide Software Private Limited harmless from any and all claims or losses relating to such unauthorized use.

9. Trademarks

LepideAuditor, LepideAuditor App, LepideAuditor App Server, LepideAuditor (Web Console), LepideAuditor Logon/Logoff Audit Module, Lepide Object Restore Wizard, Lepide Active Directory Cleaner, Lepide User Password Expiration Reminder, and LiveFeed are registered trademarks of Lepide Software Pvt Ltd.

All other brand names, product names, logos, registered marks, service marks and trademarks (except above of Lepide Software Pvt. Ltd.) appearing in this document are the sole property of their respective owners. These are purely used for informational purposes only. We have compiled a list of such trademarks, but it may be possible that a few of them are not listed here.

Microsoft®, Windows®, Windows Server®, Windows Server 2008®, Windows Server 2008 R2, Windows Server 2012®, Windows Server 2012®, Windows Server 2012®, and Windows Server 2016® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.